California AG Updates Draft CCPA Regulations (Again)

March 19, 2020

The California Attorney General has released a second set of modifications to its proposed regulations implementing the California Consumer Privacy Act. We expect that companies planning their CCPA compliance programs will want to continue to map their efforts to the evolving regulations–though the serial revisions from the AG's office do not make such mapping easy.

The good news is that the core rights and obligations defined by CCPA, and by prior iterations of the draft regulations, remain largely unchanged. Consumers' rights to know, delete, and opt out of the sale of their personal information are still the heart of the matter. And as noted below: for now, anyway, the AG's office has declined to delay the impending finalization of the regulations - or the enforcement of CCPA - despite business concerns that COVID-19 disruptions may make compliance unrealistic, and enforcement unfair.

What's new? This latest release does include a few noteworthy changes—and undoes some changes proposed by the AG's office just last month, as covered in our previous update:

- **Scope of Personal Information**: Perhaps the most significant change in the AG's new modifications is the restoration of a broader interpretation of what constitutes "personal information" under CCPA. Last month, the AG proposed an important narrowing clarification: "personal information," the AG said then, would ***not*** include IP addresses that a business does not and could not reasonably link with a particular consumer or household. The AG has now eliminated that narrowing interpretation. IP addresses thus would seem to be back in scope in the AG's view–regardless of whether a business does or can link the addresses to anybody.

  The CCPA itself still states, in section 1798.140(o)(1), a requirement of "reasonable" linkability between an IP address and a particular consumer or household before the address can qualify as "personal information." But this latest change in the draft regulations suggests the AG will read that requirement broadly, erring on the side of treating IP addresses as a form of PI. The AG's intended focus would seem to be

whether the link to a consumer or household ***could*** be drawn, not whether a particular business ***actually draws*** the link or is capable of doing so.

The change should not affect the sharing of threat information, which often includes the sharing of IP addresses thought to be associated with malicious activity. Businesses remain free to share personal information in cooperation with law enforcement, and to share information when (as is often the case with threat data) they do not receive consideration for doing so.

- **"Do Not Sell" Button**: The AG also has deleted its visual example of what a compliant "Do Not Sell" button might look like. The AG's office made this deletion after receiving comments that the toggle-style example it provided just last month could confuse consumers as to whether they have already opted out of the sale of their data. The current draft not only deletes this previously provided example, but also fails to provide any replacement guidance.

The new release also includes some notable additions:

- **Privacy Policy Contents**: The new modifications include additional requirements for the content of a privacy policy, including (i) that a business identify the ***categories of sources*** from which it collects personal information and, much like GDPR's requirement that a business identify processing purposes, (ii) that a business identify the "***business or commercial purpose*** for collecting or selling personal information." The text of CCPA provides that consumers have the right to request that a business disclose the categories of sources from which the business collects personal information and the business purposes for collection. See CCPA, §1798.110 (a)(2)-(3) & (c)(2)-(3). The draft regulations now go a step further and require that a business include this information in its privacy policy.

- **Notice at the Point of Collection**: Under the modified draft regulations, if a business collects personal information but does not do so directly from a consumer, it no longer has an obligation to provide notice at the point of collection. The catch is that, in this scenario, the business cannot sell the collected personal information. Presumably, if A acquires C's data from B and wants the right to sell that data eventually, A could still advise C at the point of the acquisition from B.

  In addition, for employee-related data, the new modifications no longer require the notice at the point of collection to include a link to the business's privacy policy.

- **Service Provider Exemptions**: The new modifications set additional limitations on third-party service providers' use of personal information. For example, the new modifications still allow service providers to use personal information "to build or improve the quality of [their] services," but now indicate that this exemption does not include "modifying household or consumer profiles ***to use in providing services to another business***, or ***correcting*** or augmenting data acquired from another source.

- **Responses to Consumer Requests to Know**: Under the new modifications, a business that receives requests to know ***should inform*** consumers if they collect sensitive personal information like Social Security numbers, driver's license numbers, other government-issued identification numbers, financial account numbers, health insurance or medical identification numbers, account passwords, security questions and answers, or unique biometric data. As noted in the prior drafts of the regulations, businesses ***should not***, however, actually disclose such information in response to a consumer request.

- **Personal Information of Minors**: If a business has actual knowledge that it sells the personal information of minors under the age of 16, the new release requires that the business describe in its privacy policy its plan for obtaining affirmative, opt-in consent for the sale of personal information–either from the parent if the minor is under the age of 13, or from the minor if between the ages of 13 and 16.

- **Reporting**: Under the new modifications, a business that "***knows or reasonably should know***" that it buys, receives, sells, or shares for commercial purposes, the personal information of 10,000,000 or more consumers in a calendar year, must disclose (i) the number of requests the business received, complied with, and denied; (ii) the number of requests to delete the business received, complied with, and denied; (iii) the number of requests to opt out that the business received, complied with and denied; and (iv) the median or mean number of days within which the business substantively responded. A business subject to this reporting requirement must make the necessary disclosure by July 1 of each calendar year.

The California Attorney General is accepting comments through March 27, including via email to PrivacyRegulations@doj.ca.gov.

Businesses might reasonably ask:

When, at last, will we have final regulations? It is tough to plan for compliance against a moving target. Unfortunately, the AG's office has not indicated when it will issue regulations in final form. The statutory deadline for adoption of regulations

remains July 1, 2020. It also remains the case that the AG cannot begin enforcement actions before July 1.

Notably, in a recent letter to Congress, AG Xavier Becerra made no promises of a final issuance date for the regulations. Instead, he simply reiterated the July 1 statutory deadline. The thrust of that letter, by the way, was to urge Congress to treat CCPA as "a floor, not a ceiling" when considering federal privacy legislation. Whether federal legislation would preempt CCPA and comparable state laws remains a hot-button issue, and an obstacle to any adoption of a federal bill.

Will there be any relaxation of deadlines or enforcement given the disruptions caused by COVID-19? Prior to the COVID-19 pandemic, AG Becerra had publicly suggested that following the law's January 1, 2020 effective date, there would be "aggressive, early, decisive enforcement action"—likely focused on children's data, and on sensitive data such as healthcare information and Social Security numbers. Media reports indicate that a number of major advertising groups have just reached out to the AG's office to ask for a delay of enforcement until Jan. 2, 2021. The groups cite both the disruptions that COVID-19 is wreaking on the private sector, as well as the unsettled status of the regulations. The same groups have previously asked the AG for a delay, without success, prior to the coronavirus outbreak.

Via *Forbes*, the AG's office has replied: "Right now, we're committed to enforcing the law upon finalizing the rules or July 1, whichever comes first. We're all mindful of the new reality created by COVID-19 and the heightened value of protecting consumers' privacy online that comes with it. We encourage businesses to be particularly mindful of data security in this time of emergency."

As always, we would be pleased to discuss these issues with our clients and friends.

* * *

Please do not hesitate to contact us with any questions.

WASHINGTON, D.C.

Jeffrey P. Cunard
jpcunard@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com

NEW YORK

NEW YORK

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Avi Gesser
agesser@debevoise.com

Henry Lebowitz
hlebowitz@debevoise.com

NEW YORK

Jim Pastore
jjpastore@debevoise.com

NEW YORK

Lisa Zornberg
lzornberg@debevoise.com

NEW YORK

Kate Saba
ksaba@debevoise.com